

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 3-7, 9-13, 15, 16 and 18-20 are pending in the present application. Claim 21 is canceled by the present amendment. No new matter is added.

In the Office Action, Claims 1, 3-7, 9-13, 15, 16 and 18-20 were rejected under 35 U.S.C. §103(a) as unpatentable over Timmer (U.S. Pub. 2002/0107895) in view of Shurts (U.S. Pat. 5,572,673).

Applicant respectfully traverses this rejection as independent Claims 1, 7, 13, 16, 19 and 20 recite novel features clearly not taught or rendered obvious by the applied references.

Independent Claim 1, for example, recites, a mobile information communication device which supports information exchange and fostering of human relations between a plurality of users, comprising:

...a metadata storage unit which stores... metadata relating to activities and interests of a user of the mobile communication device, said metadata includes **a log providing information on locations visited by the user;** and

a central control unit ..., wherein said central control unit:
partitions said metadata storage unit by security level and category,
stores metadata received through said wireless communication unit **in a corresponding partition of the metadata storage unit based on matching the received metadata with a security level and/or category** predetermined by the user, and

supplies, in response to an external access request, **metadata from the metadata storage unit that matches a security level available to the external access request.**

Independent Claims 7, 13, 16, 19 and 20, while directed to alternative embodiments, recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1, 7, 13, 16, 19 and 20.

In rejecting the claimed features directed to the “*metadata storage unit that stores... metadata including a log providing information on locations visited by a user,*” the Office Action relies on Timmer.

Timmer describes a method for creating a personalized book including content of a user’s choice, such as streaming video and interactive content, in a structure designed by the user.¹ More particularly, Timmer describes a interface that allows users to access content from various sources, or provide the content themselves, and assemble the content into a personalized book format.²

Timmer, however, fails to teach or suggest that his device used to host the book includes a *metadata storage unit that stores... metadata including a log providing information on locations visited by a user*, as recited in Claim 1.

In rejecting this claimed feature, the Office Action relies on paragraphs [0004-0006] of Timmer, noting that cited portion of the reference shows “that the data is stored on the Host.” This cited portion of Timmer does, in fact, describe that user selected content may be arranged by the user and made accessible to others from the host, which may be a personal digital assistant (PDA)³, for example. Further, Timmer describes that the content retrieved and organized by a user may be in the form of traditional Web pages, digital pictures, audio and streaming video, etc. Timmer, however, fails to teach or suggest that data is stored on the host as *metadata*, whatsoever.

Moreover, Timmer fails to teach or suggest storing metadata that includes *a log providing information on locations visited by a user*, as recited in Claim 1. In rebutting this previously presented argument, the Office Action cites paragraph [0031] of Timmer asserting that the features of “MYTRAVELBOOK” read on the above noted claimed feature. This

¹ Timmer, Abstract.

² Id., paragraph [0024]

³ Id., paragraph [0019].

cited portion of Timmer describes that a user may select content from the host and/or import content from other sites, which may be saved in a travel planning scrapbook that includes various user-entered information items regarding a specific destination. The scrapbook may then be accessed by a user during the trip to both update the scrapbook and obtain information about the destination. Timmer, however, fails to teach or suggest that any of the stored data is *metadata*, whatsoever. Further, Timmer describes that “MYTRAVELBOOK” is used as a “planning guide” to plan a trip, which has not yet occurred, and is not *a log providing information on locations visited by a user*.

Independent Claim 1 further recites that the mobile information communication device includes a central control unit that “*partitions said metadata storage unit by security level and category...stores metadata received through said wireless communication unit... based on matching the received metadata with a security level and/or category predetermined by the user... and supplies... metadata from the metadata storage unit that matches a security level available to the external access request.*”

In rejecting the above-noted claimed features, the Office Action concedes that Timmer “does not explicitly talk about details of enforcing security.” In an attempt to remedy this deficiency, the Office Action relies on Shurts.

Shurts describes a database management system used to provide security for database objects. More particularly, Shurts describes that a mechanism for “certifying” that certain types of objects such as stored procedures, triggers, and views can be safely used to access other sensitive objects in the database.⁴

In rejecting the above-noted “storing” and “supplying” features recited in independent Claim 1, the Office Action relies on col. 5, ll. 7-20 of Shurts. This cited portion of Shurts defines the term “dominance” and describes that the term refers to a relationship between a

⁴ Shurts, Abstract.

subject and an object specifying whether the subject can access the object. In a MAC policy, a subject is permitted read access to an object when the subject "dominates" the object. Conversely, a subject is permitted write access to an object when the object dominates the subject. Shurts further describes that write access is granted only if the subject's write sensitivity label is equal to the object's access sensitivity label.

Thus, the cited portion of Shurts merely uses "dominance" to determine when an subject is permitted access to an object, or vice versa. Claim 1, on the other hand, uses a security level to *partition a storage unit and store metadata...* in a corresponding partition of the metadata storage unit *based on matching the received metadata with a security level and/or category predetermined by the user*. Such a process of partitioning a storage unit and storing metadata in a corresponding partition of memory by matching the metadata to a category predetermined to a user, is in no way analogous to using a "dominance" level to determine if a database subject is permitted to access an object as described by Shurts.

Further, Shurts fails to teach or suggest a process of *supplying* data, whatsoever, much less "*suppl[ying]... metadata from the metadata storage unit that matches a security level available to the external access request,*" as claimed. In contrast, and as discussed above, Shurts merely describes a process of determining when an object in a database may be accessed.

Therefore, Timmer and Shurts, even if combined, fail to teach or suggest a mobile information communication device including "*a metadata storage unit which stores... metadata includ[ing] a log providing information on locations visited by the user,*" and a central control unit that *partitions a metadata storage unit, "stores metadata...* in a corresponding partition of the metadata storage unit *based on matching the received metadata with a security level and/or category predetermined by the user... and supplies...*

metadata from the metadata storage unit *that matches a security level available to the external access request,*" as recited in independent Claim 1.

Accordingly, Applicants respectfully submit that Claims 1, 7, 13, 16, 19 and 20, and claims depending therefrom, patentably distinguish over Timmer and Shurts considered individually or in combination.

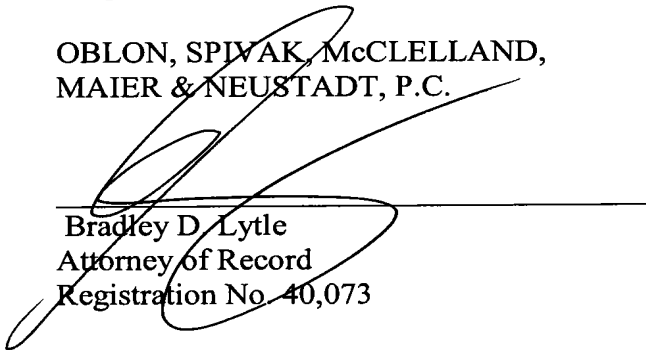
Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3-7, 9-13, 15, 16 and 18-20 is definite and patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959